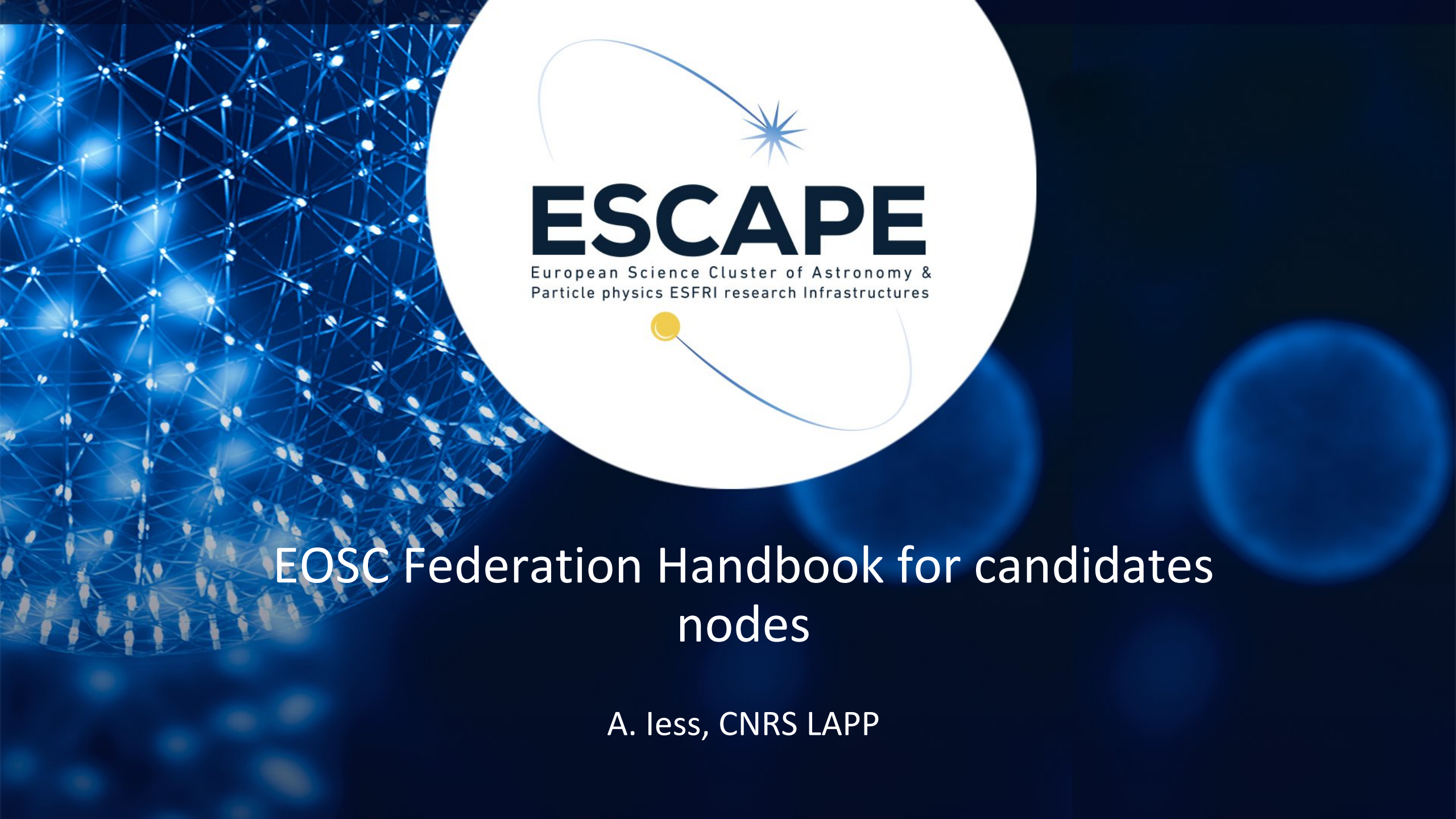


EOSC Federation Handbook for candidates nodes

A. Iess, CNRS LAPP

EOSC Federation Handbook for candidates nodes

Chapter 1 lays the foundations on which the rest of the Handbook is built. It includes the purpose of the EOSC Federation, its primary users, its main advantages and expected outcomes and success criteria.

Chapter 2 concerns the governance framework and legal structure. It describes the governance structure in its current state, communication and relations with other initiatives, and how to manage possible risks. Chapter 2 identifies governance roles for the Federation as well as for candidate Nodes.

Chapter 3 defines and describes the operational structure of the EOSC Federation. The requirements to become an EOSC Node, technical or otherwise, are outlined here.

Chapter 4 details the architecture of an EOSC Node, how services can be set up and interlinked, and specifically the requirements for federated capabilities and relationships with the EOSC EU Node.

Chapter 5 contains a description of the different categories of FAIR data and scientific resources that can be made available through the EOSC Federation.

Chapter 6 describes the process of enrolling an EOSC Node and onboarding a service in an existing EOSC Node.

EOSC Federation Handbook for candidates nodes

FROM CHAPTER 2:

"*The EOSC Nodes will need to comply with decisions, rules and policies that are agreed to be applied across the EOSC Federation.*"

Each EOSC Node will be fully autonomous to set its own rules (e.g. specific onboarding requirements, separate access/use policies) and internal management of its consortium as long as they do not contradict those of the EOSC Federation.

"*An EOSC Node can consist of a single organisation, or a consortium of organisations with its own internal governance structure. In the latter case there must be a 'coordinating' organisation within the consortium that will represent the Node in the EOSC Nodes Forum*". —> EOSC Nodes Forum advises the EOSC Tripartite Governance and the EOSC Association on issues related to the EOSC Federation activities and priorities.

EOSC Federation Handbook for candidates nodes

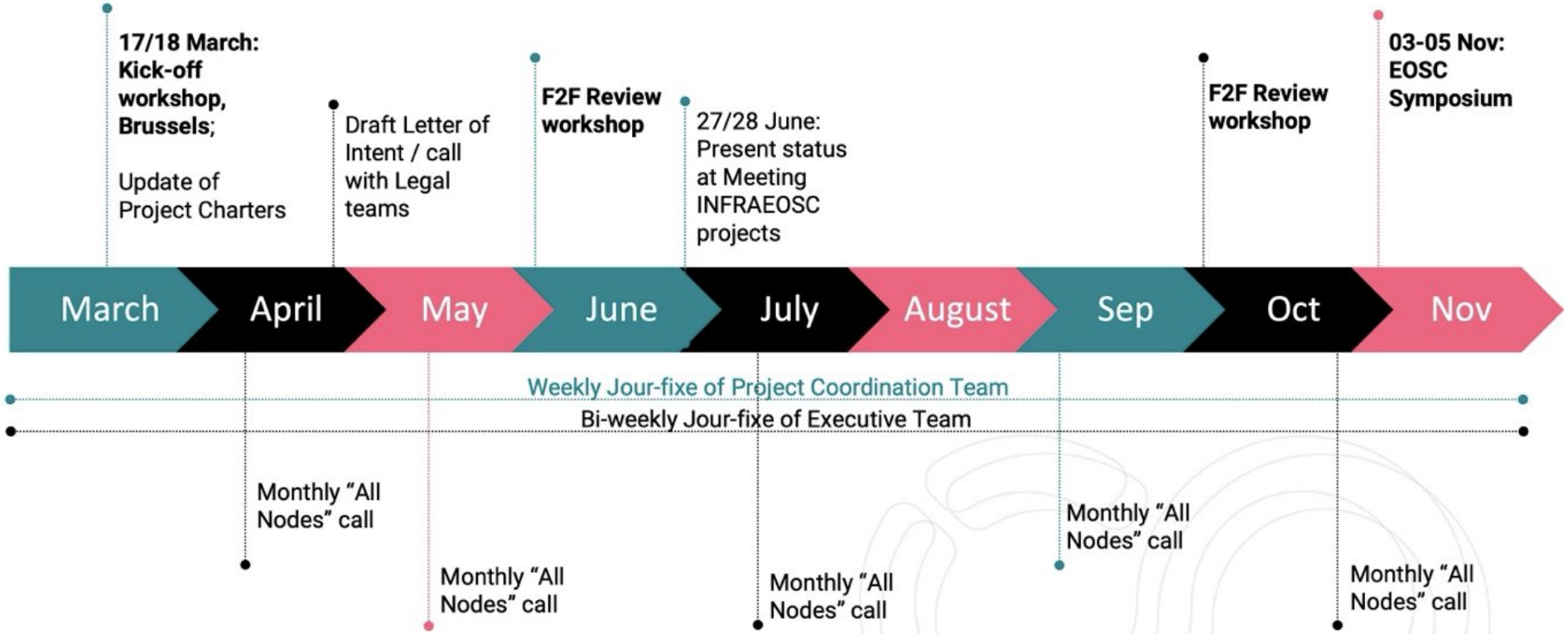
FROM CHAPTER 2:

"the EOSC Federation bodies, i.e. the EOSCTripartite governance and the EOSC Nodes Forum, will develop":

- **Federation strategy**: defining the long-term objectives of the EOSC Federation and the roadmap for achieving them.
- **Membership:** selection criteria and process for enrolment of new Nodes, their ongoing obligations, compliance measures, removal and mechanisms for appeal, possible membership fees.
- **Federated services**: common services that will be implemented across the EOSC Federation and the requirements for the Nodes when participating in federated services. These can include e.g. a common EOSC Authentication and Authorization Infrastructure (AAI), a common catalogue of EOSC resources etc.
- **Technical standards and requirements**: which technical standards will be part of the EOSC Interoperability Framework and what the technical requirements will need to be fulfilled by the Nodes when joining the Federation, e.g. cyber-security, Persistent Identifiers (PIDs) etc.
- **Federation policies**, for example a security policy, ethics policy, or Rules for Participation and policies related to the access and use of resources that are provided across the Federation.
- **Monitoring**: mechanisms to measure the Key Performance Indicators (KPIs) listed in chapter 1.
- **Collaborations**: establishing partnerships or other forms of cooperation with other organisations in and beyond Europe.
- **Governance:** what should be the characteristics of the bodies of the eventual EOSC governance, their roles and the relations amongst each other.
- **Service Level Agreement** (SLA), including the terms of the service expected from providers and precautions and actions to be undertaken in the case the terms of the SLA are not met.

EOSC Federation Handbook for candidates nodes

eosc Tentative Timeline for build-up phase of the EOSC Federation



EOSC Federation Handbook for candidates nodes

FROM CHAPTER 3:

EOSC Node will be typically formed by multiple research institutes, universities and otherstakeholders with a common geographical (European, regional or national) or thematic scope.

- Basic Requirements document (May 2024).
- Will be formalised as the “Rules of Participation for EOSC Nodes”.
- Will specify the eligibility and evaluation criteria for an organisation that isinterested in operating an EOSC Node.

EOSC Federation Handbook for candidates nodes

EOSC Federated Resources provisioned by Node itself, members of the community associated with the Node or third-party providers. Must comply with technical and operational requirements, such as those defined in:

- EOSC Interoperability Framework
- EOSC Rules of Participation for the EOSC Exchange

A non-conforming Node will be asked to address any issues identified and may be subject to suspension from the Federation.

EOSC Federation Handbook for candidates nodes

EOSC Node Cybersecurity

- Ensure compliance with regulations, standards, and best practices.
- Define roles, workflows, and security controls.
- Handle and report non-compliance properly.
- Establish a security framework (use ITSRM², ISO/IEC 27000).
- Perform regular risk assessments and implement protections.
- Monitor, review, and improve security measures.
- Set up a CSIRT for incident response and reporting.
- Provide access control via Federated AAI and SSO.
- Protect data (minimisation, encryption, privacy by design).
- Offer continuous security training and awareness.

EOSC Federation Handbook for candidates nodes

EOSC Node Technical Operations

- EOSC Nodes must implement a Service Management System (SMS) following standards like FitSM or ISO-20000 and ITIL best practices.
- SMS ensures service levels agreed with EOSC Federation and service providers are met.
- Service levels must cover provisioning, integration, monitoring, support, quality, and change management.
- Nodes without an SMS should adopt FitSM, well-suited for federated services.
- EOSC EU Node's SMS can be used as a reference model.

EOSC Federation Handbook for candidates nodes

3.2.3 Roles for EOSC Nodes

In order to facilitate the interaction of the Node with the Federation, each Node must nominate a number of persons in the following roles:

1. A **Coordinator** who represents the Node in the Federation.
2. An **Operation Manager** who is the contact person with the Operations Team of the Federation on operations.
3. A **Technical Coordinator** who is the contact person with the Technical Coordination Team of the Federation on technical issues (mainly IT issues).
4. A **Security Officer** who is the contact person for all security related issues.
5. Thematic Nodes will nominate a **Scientific Officer** who represents the Node's scientific content.
6. A **Legal/Privacy Officer** for legal issues

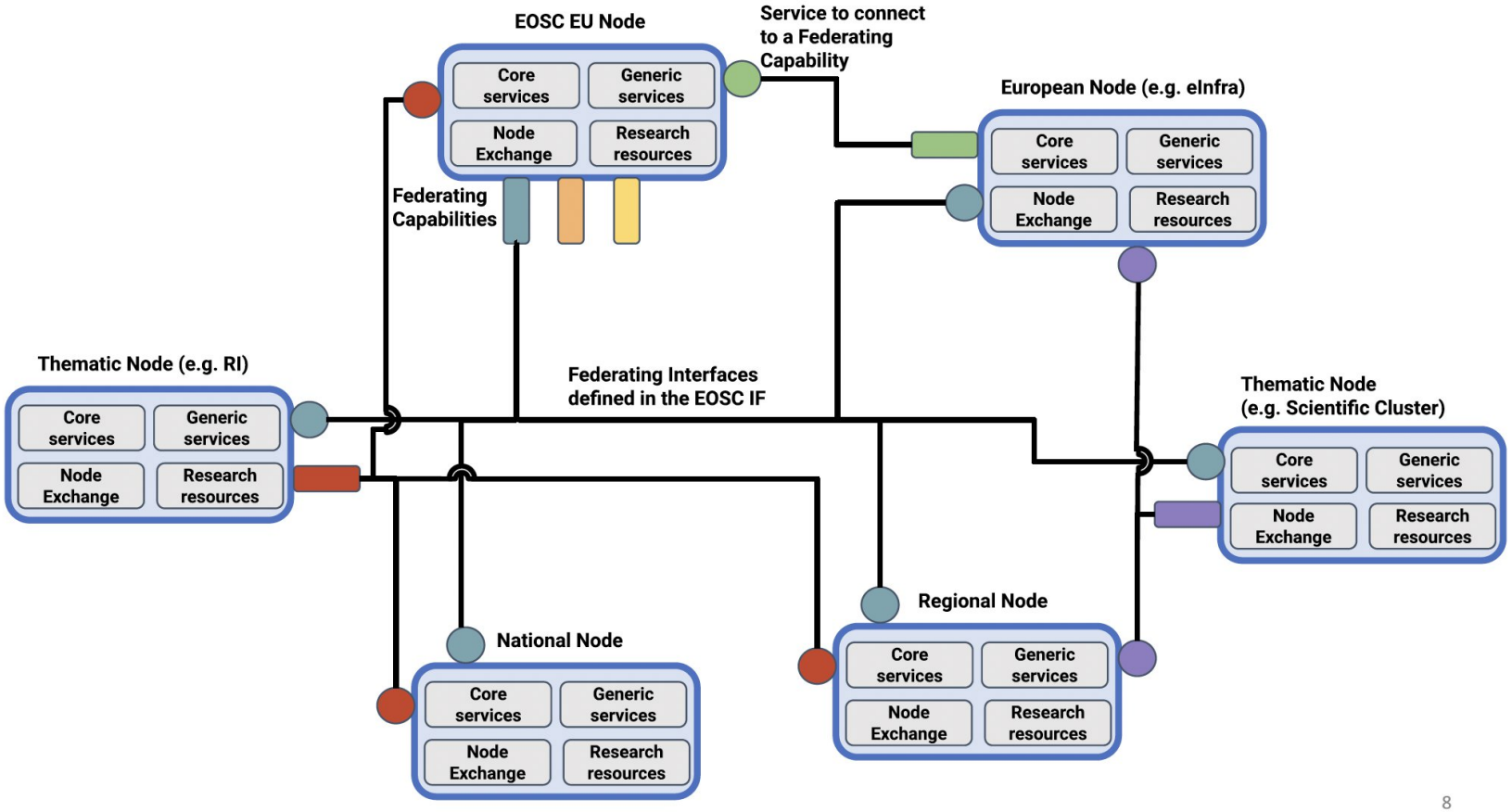
The Node will nominate the persons in these positions once the Node has been accepted to join the Federation and will communicate their names to the Operations Team of the EOSC Federation.

EOSC Federation Handbook for candidates nodes

FROM CHAPTER 4:

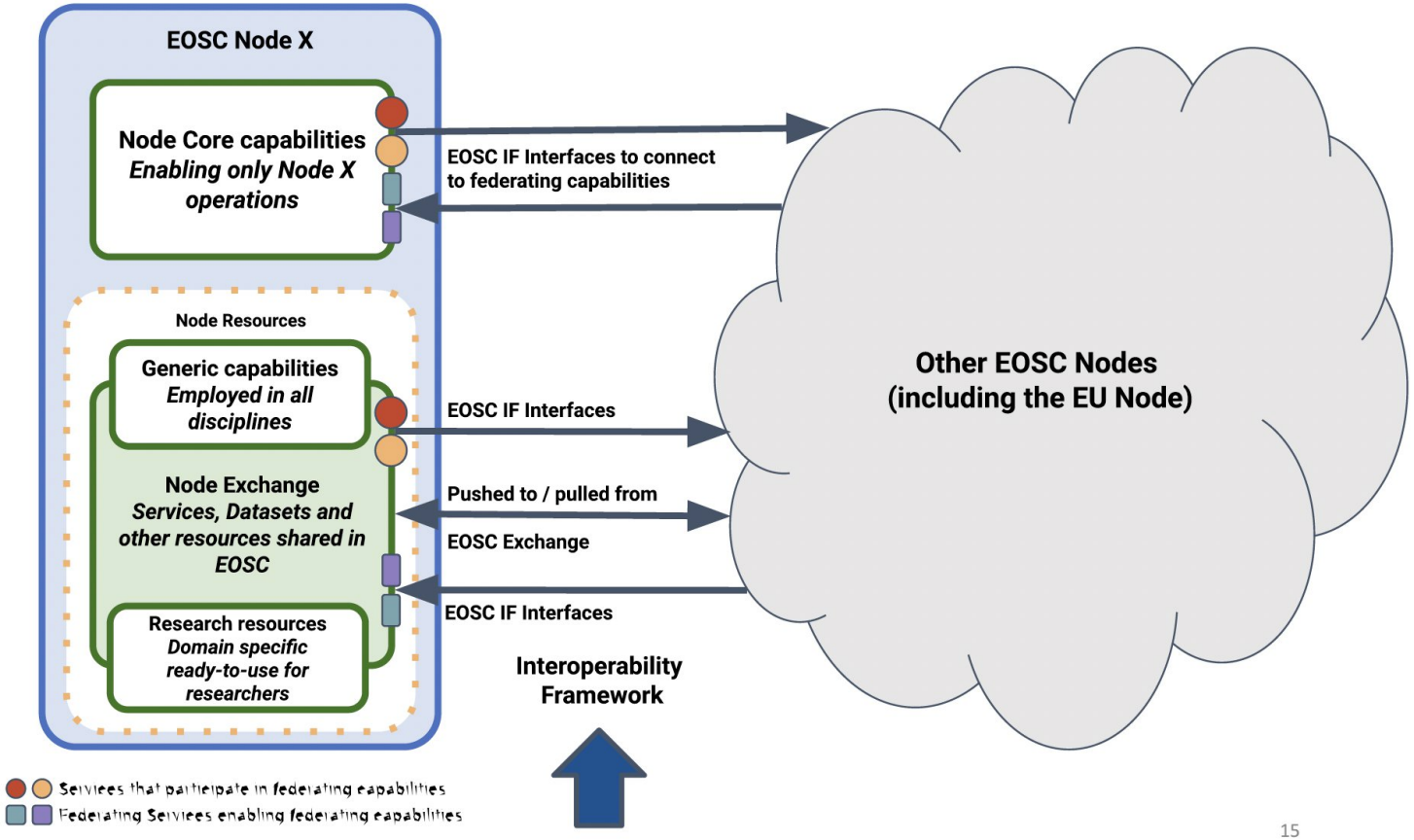
- **EOSC Nodes (blue boxes)**
- Additional capabilities that allow end-users and providers to exploit services, data and other resources in the Federation, referred to as **Federating Capabilities (coloured "sticks")**, enabled by one or more Federating Services provided by the EOSC Nodes;
- **interfaces (black lines)**, comprising APIs and metadata schemas, that connect Node services (shown as coloured "circles") to the Federating Capabilities.

"The capabilities define in practice an integrated digital platform that can be realised with the tools of preference of the communities engaged in the EOSC Nodes."



EOSC Federation Handbook for candidates nodes

- Node Core Capabilities.
- Node Resources (Node Generic Capabilities [data tansfer, cloud infrastructure], Node Research Resources, **Node Exchange**).
- Services enabling Federating Capabilities.



EOSC Federation Handbook for candidates nodes

4.2.2.2 Node Exchange

The EOSC Federation expects EOSC Nodes to make a relevant portion of their resources available to the rest of the EOSC Federation under the appropriate User Access Policy. The decision of which Node Resources are made available will be taken by the Governance of the Node, and/or the providers of specific resources. Resources shared with the Federation will be labelled by the EOSC Node as **Node Exchange** and they will be discoverable, accessible and usable by any EOSC User[20] according to the conditions laid out in the respective Access Policies decided by the EOSC Nodes. They will therefore have to comply with the EOSC Federation Policies. Other services and resources that are *not* made available in the EOSC Federation do *not* need to be compliant with the EOSC Federation Policies.

In the Node Exchange, we can identify either resources which are generic by nature enabling capabilities and resources which can be used by the majority of research communities and researchers (e.g. Generic Capabilities, see section 4.2.2.1) or resources that are more science-/domain-specific, for example, domain-specific notebooks/workflows, virtual research environments, datasets and/or research software. Chapter 5 provides more information about the scientific research services and resources which can be provided by EOSC Nodes via the EOSC Federation.

Node Core Capabilities

Node Core Capabilities	Description
Resource Catalogue and Registry services	Catalogue of resources that can be accessed through the EOSC Node with a search engine to discover, access and order them
AAI	AAI (AARC Blueprint- compliant) enabling access to Node resources (Core and Exchange) via federated credentials (i.e. community AAI and Infrastructure Proxy)
Helpdesk	Support incident response and service requests for services and other integrated resources
Service Monitoring	Monitor the availability and quality of the Node services
Service and Research Product Accounting	Track and record usage of resources
Order Management	A framework for providers to define offers and a unique interface for end-users to request access to resources
Configuration Management System	Shared space to store information on Node capabilities and on how services are provided through the node to ensure consistent service delivery (only for internal use)
User space	Dynamic customisable dashboard, where the node user logs-in, offering easy access to the Node resources.
Application Workflow Management	Orchestrate services, datasets and other research objects on the underlying Node provisioned infrastructure
Resource provisioning	Support users on identifying all available resources for a project and then assigning them to the project

Node Generic Capabilities

Node Capabilities	Description
Data Transfer	Transfer of data between storage locations
Notebooks	Support for data analysis
Compute and storage resources (including middleware)	Support for data analysis with relevant middleware (e.g. support for containers)
File Sync & Share	Syncing automatically data across devices (e.g. PCs, tablets, or smartphones) and securely sharing them within research teams

EOSC Federation Handbook for candidates nodes

EOSC Federating Capabilities

Federating Capability	Description	Classification
Resource Catalogues and Registry services	• Federated EOSC Resource Catalogue making the Node exchange resources discoverable • Search engine over the whole EOSC Federation • Interfaces to allow EOSC Nodes to publish (push) and retrieve (pull) resources to/from the federated catalogue	Mandatory
AAI	Allows users to log in with their own institute credentials (eduGAIN) to access EOSC resources	Recommended[24]
Application Workflow Management	Orchestrate services, datasets and other research objects on multiple federated nodes	Recommended
Service Monitoring	Provide information about the availability and quality of EOSC services (Core and Exchange)	Recommended
Service and Research Product Accounting	Provide information about usage of services and resources in EOSC (Core and Exchange)	Recommended
Order Management	Offer a framework for providers to define offers and a unique interface for end-users to request access to resources	Recommended
Helpdesk	Federation of integrated helpdesks	Recommended
Management System	FitSM-based Service Management System (SMS) that can be federated with SMS from other EOSC Nodes. This includes Security Coordination between Nodes too.	Recommended

Research Resources Categories

Resource	Category	Description
Research Competence Centres	Mentoring	A Competence Centre (CC) is a virtual hub dedicated to fostering research excellence through training and knowledge transfer. The CCs are community-based initiatives supported by a collaborative network of people providing expertise, best practices and services in relation to Open Science, and the promotion of cross-disciplinary collaboration
Research Resources and Services Discovery	Service	Search engine for research resources and services for domain specific searches tuned for researchers

Resource	Category	Description
Research Publications	Publications	Textual output of scientific research that gives the possibility of verification of research findings or their use in new research; mostly but not only refers to peer reviewed publications in journals, can also be publications that are not peer reviewed (such as preprints)
Research Data sources	Data	Sources where data can be found and retrieved, offering APIs or direct access to data searches across various query fields. Data repositories and archives, knowledge bases and scientific databases fall into this category
Research Data	Data	Data from scientific research; referenced by a PID; following the FAIR guidelines as best possible
Research Software	Software	Software for simulating, generating, processing and analysing research data. This includes notebooks and workflows. Software is referred to via a software PID
Research Tools	Software	Analytical and visualisation and other types of tools to aid in the interpretation, transformation and presentation of data. These tools may include dashboards, plotting software, data anonymization software and machine learning frameworks
Research Services	Products	Services that provide management, processing, and storage capabilities for research data. These may include DMPs, data cleaning, transformation, analytics, and computational power to support large-scale studies
Research Training	Documentation	Educational resources designed to improve data literacy, technical skills, and knowledge of best practices in all aspects relevant to EOSC. This includes structured courses and schools, webinars, and hands-on workshops
Research Interoperability guidelines	Documentation	Guidelines to ensure compatibility and seamless data exchange between systems. This category includes metadata standards, data-sharing protocols, and frameworks for harmonizing metadata and data formats

EOSC Federation Handbook for candidates nodes

EOSC build up next wave will be carried out in mid-2025 (?). The EOSC Nodes Requirements draft defines minimal requirements:

- **Legal status** with full capacity to conclude agreements with partners, other nodes, and potential future organisation representing EOSC Federation.
- **Large-scale quality service provision.**
- **Capacity to onboard third party services.**
- **Capacity to contribute to EOSC Core Capabilities (AAI, helpdesk, monitoring, catalogues, registries, accounting).**
- **Compliance with EOSC Federation rules and standards.**
- **Effective monitoring of its services.**
- **Community engagement.**
- **Sustainability (continuous EOSC Fedeartion-compliant operation of services for at least 5 or more years).**

EOSC Federation Handbook for candidates nodes

Legal organizational steps

The node partners need to agree on how they will manage themselves and how they will comply with the policies of the EOSC Federation. At a minimum they will need to sign a Memorandum of Understanding that defines the role and responsibility of each partner. In some cases, partners could be required to sign a contract which defines the specific rules and regulations governing the EOSC Node. It is up to each node to decide how to manage themselves and will depend on the links existing between the partners and providers or resources which will be onboarded.

Once a node is accepted to be part of the EOSC Federation it will need to sign a legal agreement with the EOSC Federation Management Organisation which describes the conditions and policies of the EOSC Federation Nodes must comply with. The exact form of the agreement is not decided yet and will be added here once it is known.

Policies procedural steps

The EOSC Federation needs to ensure that all its members i.e. all EOSC Nodes, comply with a common set of policies concerning the different aspects which are considered to be part of the Federation e.g. privacy, cybersecurity, data, user access etc. The exact list of policies is not known yet but a document containing proposals produced during the writing of the Handbook could serve as the starting point. The list of policies will be updated here once they have been decided by the EOSC Federation Governance.

EOSC Federation Handbook for candidates nodes

8 Annex 2 - Recommended Guidelines

The goal of the EOSC Federation is to ensure that EOSC Nodes provide high quality resources by implementing a set of recommended guidelines. The EOSC Federation Handbook currently recommends adopting the following guidelines:

1. "**Guidelines for creating a user tailored EOSC Compliant PID Policy**" by FAIR-IMPACT (https://doi.org/10.5281/zenodo.14092489)
2. "**Guidelines for recommended metadata standard for research software within EOSC**", produced by FAIR-IMPACT (https://doi.org/10.5281/zenodo.10786147)

The following guidelines are required but currently missing and should be produced in the future by the expert groups working projects or as part of the EOSC Association Taskforces activities:

3. ***Trustworthiness of data repositories*** - guidelines should follow on the work by FAIR-IMPACT and FIDELIS INFRAEOSC projects
4. ***Machine actionable data access*** - guidelines needed to describe how machine will access research data.

Technical Steps to set up an EOSC Node

Steps		Description
1	**Compliance with the EOSC Node reference**	The digital infrastructure behind each Node of the EOSC Federation should offer services and other resources to its users with an adequate
2	**Professionally operate the digital infrastructure (Mandatory)**	EOSC Node digital infrastructures should implement a Service Management System based on IT Service Management (ITSM) standards for their Technical Operations (see Section 4.5) and ensure Cybersecurity (Section 4.6).
3	**Publish/expose resources in/to the EOSC Federation Catalogue (Resource Hub) (Mandatory)**	Each Node must identify its Node Exchange selecting a subset of resources (services, datasets or other research products) that can be discovered and accessed by EOSC users under proper AUPs. Resources in the Node Exchange must be published in the EOSC Federation Catalogue operated by the EOSC EU Node (Resource Hub - Tier 3). Details on how to register resources in the EOSC EU Node Resource Hub are reported in Annex 1.
4	**Access to the Node resources via eduGain IDPs (Mandatory)**	Each node must operate an AARC Blueprint compliant AAI infrastructure made up of a Community AAI and an Infrastructure Proxy. The Node also needs to join the eduGAIN Federation as Service Provider[52].
5	**Connect to existing Federating Capabilities (Recommended)**	Each Node should analyse the Federating Capabilities of the EOSC Federation, connect its services to the mandatory ones, and select with which of the recommended ones it would like to federate. To connect, EOSC Nodes should follow the instructions of the relevant Interoperability Guidelines. Nodes can use technologies of choice or the reference implementation delivered by the EOSC EU Node to connect (see Annex 1). The list of the Federating Capabilities available in the EOSC Federation are listed in Table 4.3 of Section 4.3.1.
6	**Enable new Federating Capabilities (Optional)**	Each Node can decide to enable new Federating Capabilities in the EOSC Federation in accordance with the EOSC Federation Governance.

EOSC EU Node Federating Capabilities

Resource Catalogues and Registry services	
Description	Catalogues that provide resource records to the EOSC EU Node and the EOSC Resource Hub and interfaces for resource publication and harvesting. The EOSC EU Node Service Catalogue include 3 different categories: • **Tier 1 - EU Node native services:** Core and Generic services directly funded by EC through procurement; • **Tier 2 - Services onboarded in the EOSC EU Node:** after onboarding via the appropriate process, these services are expected to be integrated with the EU Node Core services, respecting similar service level agreements; • **Tier 3 - Services and Research Products discoverable in the EOSC EU Node Resource Hub:** resources registered in other EOSC Nodes made discoverable in the EOSC Federation by the EU Node through the Resource Hub.
Federating Capability (enabled by this service)	**Tier 2 Services onboarded in the EOSC EU Node:** This integration option applies to providers willing to make available their resources in the EOSC EU Node. It is expected that this option would require a tight integration with the EOSC EU Node. Integration guidelines for this option are not available yet. **Tier 3 Resources discoverable in the Resource Hub of the EOSC EU Node:** This integration option applies to organisations willing to establish their own EOSC Node and make their services and research products discoverable in the EOSC EU Node Resource Hub (mandatory step to join the EOSC Federation, see Section 4.6). It allows to connect resource catalogues from other EOSC Nodes to the federated catalogue hosted in the EU Node to enable other EOSC Nodes to: • publish their resources in the EOSC EU Node Federated Catalogue; • retrieve and add to their catalogue resources from the EOSC EU Node Federated Catalogue.
Relevant Interoperability Guidelines	• EOSC Profiles: Guidelines for Onboarding Resources to EOSC Exchange (V5.0) • Service Catalogue: Architecture and Interoperability Guidelines • EOSC Interoperability Guidelines for Data Sources to onboard Research Products

User Space	
Description	The User Space is a web interface that allows EOSC Node users to access all the underlying services of the EU Node. It allows users to manage their profile that includes information such as identifiers, preferences, affiliations, credits, notifications, etc.
Federating Capability (enabled by this service)	Not available
Relevant Interoperability Guidelines	Not available

Identity Management	
Description	Access to the EOSC EU Node services via federated credentials.
Federating Capability (enabled by this service)	AAI federation to enable the single sign-on over multiple EOSC Nodes.
Relevant Interoperability Guidelines	• AARC Blueprint Architecture • AARC Guidelines

Application Workflow Management	
Description	The Application Workflow Management (AWM) allows EOSC users to deploy applications in the underlying EOSC EU Node cloud that have an associated deployment recipe (e.g. TOSCA templates, Ansible Playbooks, Helm charts). The AWM takes care of orchestrating applications described in TOSCA templates and Ansible playbooks, and supports their deployment defined through Helm charts, Docker compose files or other specification through Ansible commands.
Federating Capability (enabled by this service)	In addition to the EOSC EU Node Cloud, AWM can deploy applications in multiple cloud infrastructures. It offers a large and easy extensible set of interfaces and plugins, that will be soon exposed to end-users, towards public cloud providers such as Amazon EC2, Google Cloud Platform, Microsoft Azure, T-Systems OTC, Orange flexible engine, on-premises cloud management platforms such as OpenNebula, OpenStack and federated environments such as the EGI Cloud Compute. A Cloud Infrastructure can be connected to AWM using one of the available plugins, or developing an ad-hoc plugin.
Relevant Interoperability Guidelines	• Definition of virtual infrastructures for supported AWM back-end and specification of credentials for backends. • Plugins for new backends are developed by creating a new "CloudConnector" class. Detailed documentation will be available soon.

Service Monitoring	
Description	Monitoring is the key service needed to gain insights into the distributed infrastructure of EOSC. It needs to be continuous and on-demand to quickly detect, correlate, and analyse data for a fast reaction to anomalous behaviour before they affect end-users and productivity. Management teams can monitor the availability and reliability of the services from a high-level view down to individual system metrics and monitor the conformance of multiple SLAs. The Monitoring service was designed to support multiple entry points (different types of systems can work together) and be easily interoperable with other monitoring systems. The Monitoring service combines two operational monitoring services: the EOSC Core and the EOSC Exchange Monitoring Services, respectively monitoring the EOSC EU Node Core services and the services onboarded in the EU Node (tier 2 and tier 3).
Federating Capability (enabled by this service)	The Service Monitoring offers the following integration options: • *Monitor an Onboarded Service*: monitor a single EOSC Service onboarded in the EOSC EU Node (Tier 2 or Tier 3); • *Monitor an EOSC Node:* monitor a complete infrastructure (including EOSC Nodes) supporting multiple Services and Resources; • *Integrate External Monitoring service:* configure the EOSC Monitoring service to accept monitoring data from third-party monitoring engines (e.g. other EOSC Nodes); • *Combine Monitoring Results from multiple EOSC Nodes:* allow to combine the topology and the results of multiple infrastructures in a number of reports; • *Third-party services exploiting EOSC Monitoring data:* a customer retrieves results from the EOSC Monitoring Service to use them in an external service/dashboard.
Relevant Interoperability Guidelines	• EOSC Monitoring: Architecture and Interoperability Guidelines

Service Accounting	
Description	The Service Accounting is a platform designed to streamline metric collection, aggregation, and exchange across diverse infrastructures, providers, and projects. This comprehensive solution offers a REST API, empowering clients to seamlessly integrate their metrics into the system. This API accepts input from various resources, securely stores it in a database, and performs intelligent aggregation of incoming data.
Federating Capability (enabled by this service)	The Service Accounting offers the following integration options: • Integrate with an aggregator (e.g. an EOSC Node) of accounting data; • Integrate with a service provider; • Make use of the accounting data.
Relevant Interoperability Guidelines	• EOSC Accounting for Services interoperability Guideline

Research Product Accounting	
Description	The EOSC Research Products Accounting collects usage activity from events from EOSC Data sources, i.e. EOSC services that host collections of research products, like articles, books, datasets, etc. and include data repositories, software repositories, and publication repositories. The service forms metrics of usage activity of these Data sources, categorizing the data retrieved by number of downloads, number of views, number of repositories and all derivative quantitative open metrics, comprehensively. UsageCounts service provides standards for usage data exchange, it complies to the COUNTER Code of Practice for reliable and comparable reports, it respects user's privacy via IP anonymization of usage events, it offers global coverage and enables accumulation of usage for the same research products by exploiting the metadata deduplication functionality of the EOSC Research Graph.
Federating Capability (enabled by this service)	EOSC data source managers (including EOSC Nodes) can participate in the Research Products Accounting Service following the interoperability guidelines of this service (see below) that specify methods and standards used to collect and process usage data in order to generate comparable, standards-based usage statistics. The guidelines follow the Release 4 and Release 5 of the COUNTER Code of Practice for e-Resources.
Relevant Interoperability Guidelines	• EOSC IF Interoperability Guidelines for Research Products Accounting

Order Management	
Description	The Order Management Services facilitates the order processing, offering providers and communities several flexible options to integrate their own ordering process with the EU Node, enabling them to track all the orders received and to propose different actions on these orders. End-users can order resources, monitor user requests, and communicate with resource providers. Providers can specify offerings for their resources, configure their offerings using an API or ergonomic UI, handle orders placed in the system using Ordering API (integrate any existing OMSs).
Federating Capability (enabled by this service)	Not available
Relevant Interoperability Guidelines	• Order Management System Interoperability Guideline

Helpdesk	
Description	The Helpdesk is the entry point and ticketing system/request tracker for issues concerning the available EOSC EU Node services. It implements efficient communication channels between users and providers of the EU Node services.
Federating Capability (enabled by this service)	The Helpdesk offers the following integration options: • *Direct Usage:* an EOSC Node uses the EOSC EU Node helpdesk as a service with a dedicated tenant. Users of the EOSC Node can login to use the service in a dedicated area for that Node. • *Ticket redirection:* an EOSC Node uses the EOSC EU Node helpdesk as first line of support. Any ticket created in the EU Node helpdesk related to this EOSC Node will be automatically redirected by email. • *Full Integration:* an EOSC Node can integrate its own Helpdesk software with the EU Node Helpdesk, which enables full synchronisation by way of an API and is technology-agnostic of the Provider's Helpdesk solution. • *Dedicated instance:* EOSC Nodes can also deploy a dedicated instance of the Helpdesk and to integrate that with the EU Node helpdesk. This requires bilateral discussion between the EOSC Node and the EU Node Helpdesk operator.
Relevant Interoperability Guidelines	• EOSC Helpdesk: Architecture and Interoperability Guidelines

PID Service	
Description	The PID Service offers a distributed service for storing, managing and accessing PIDs, including their essential metadata (PID records). The service offers a REST API and a native Handle API supporting the HDL protocol. Both APIs can be used by middleware applications, end-user tools and other services to reliably identify data objects over longer time spans and through changes in object location or ownership. The PID namespace is organised on the basis of the PID Prefix, while the PID Suffix identifies individual objects registered within the Prefix namespace. PID Prefixes are acquired through ePIC of which the PID service providers are members of. PIDs are globally resolvable through the DONA Global Handle Registry network.
Federating Capability (enabled by this service)	The Resource Catalogue of the EOSC Node and each approved EOSC Node catalogue will receive their own Prefix to clearly identify the individual catalogues and the services onboarded within. Through the onboarding policies and processes for enrolling EOSC Nodes, the PID namespace can be coordinated and deduplication can be managed. The PID service is offered both for EOSC Nodes and service providers.
Relevant Interoperability Guidelines	Not available

EOSC EU Node Tier 1 native services

Service	Description
Compute/Storage	The EOSC EU Node offers cloud compute and storage resources to support processing, analytics, and other data and compute-intensive use cases. These resources are delivered to users and user communities via a resource discovery and resource allocation processes (i.e.VM Orchestration function) that interacts and integrates with the EOSC Core.
Containers	The Container Service enables the deployment of cloud native applications for scientific research communities on the EOSC EU Node. The container orchestration function automates the deployment, management, scaling, and networking of containers.
Bulk Data Transfer	The Bulk Data Transfer allows managing and transferring large data sets (e.g. in terabyte scale) in a reliable fashion, ensuring data accuracy and integrity.
File Sync and Share	The File Sync and Share service allows users to securely share documents, audio-visual content and other file-based resources across multiple devices and with multiple people.
Interactive Notebooks	The Interactive Notebooks services provide a powerful and flexible environment for data scientists, analysts, and developers to create, run, and share Notebooks, enabling faster iteration, better collaboration, and more efficient data exploration and analysis.
Large File Transfer	The Large File Transfer service allows end-users to transfer large files between computers or devices over the Internet.

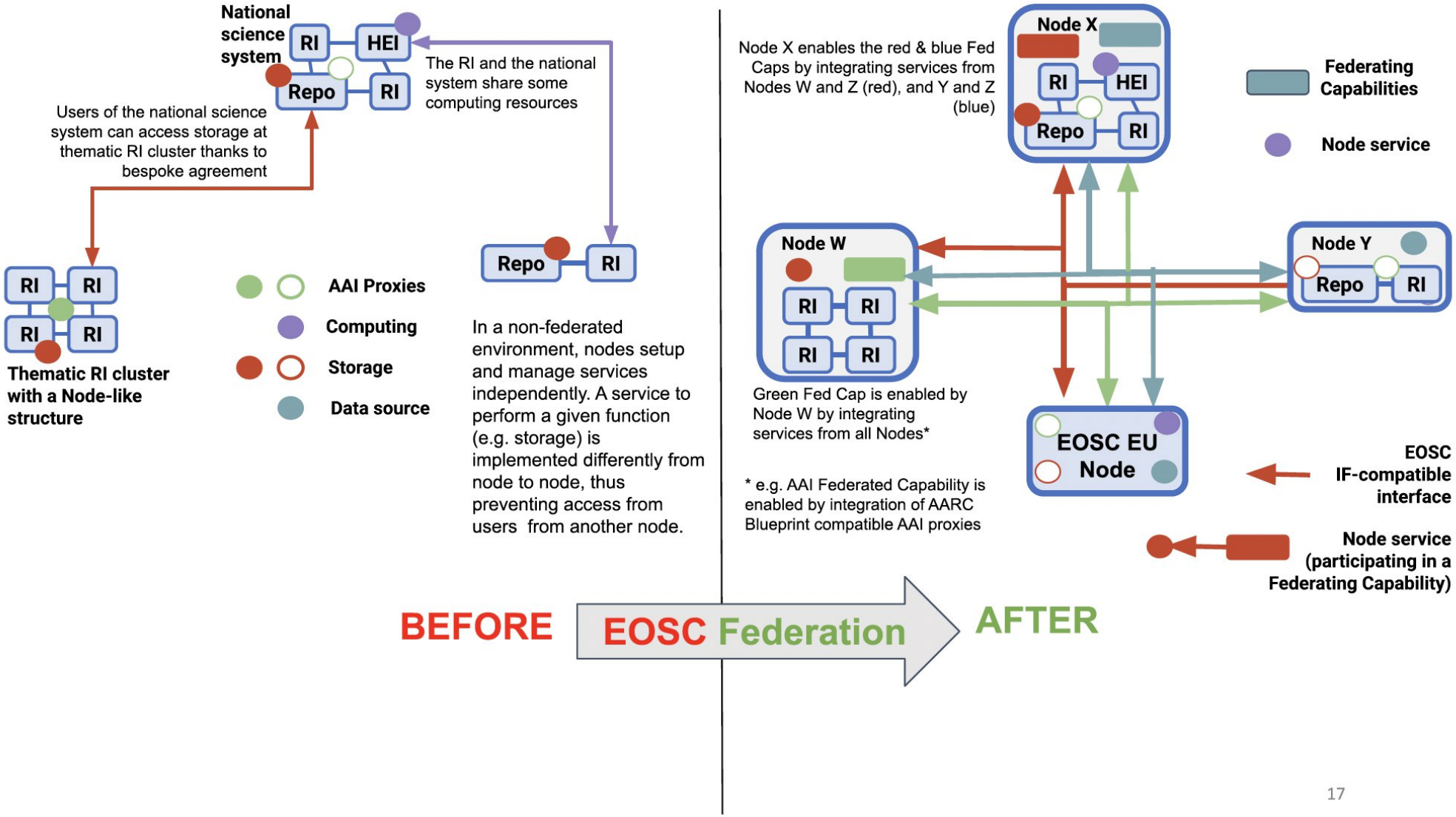


Figure 1: Before and After - Schematic showing effect of EOSC Federation on research services